



Office of the President

PO Box 3000 • Merrifield VA • 22119-3000

October 14, 2003

A handwritten number "6" enclosed within a hand-drawn circle.

Ms. Jennifer J. Johnson
Secretary of the Board
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Re: Docket No. OP-1155

Dear Ms. Johnson:

Navy Federal Credit Union provides the following comments in response to the Federal Reserve Board's proposed Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Navy Federal is the world's largest natural person credit union with over \$19 billion in assets and nearly 2.5 million members. We serve Department of Navy personnel, dependents, and family members in every state and many locations overseas.

Navy Federal understands that this proposed Guidance was developed in cooperation with the other federal functional regulators, including the National Credit Union Administration (NCUA). However, in addition to commenting directly to NCUA when its version of the proposed Guidance is issued, Navy Federal also wishes to provide its comments now during this initial comment period.

While Navy Federal currently makes a concerted effort to ensure our members' information is secure, we also acknowledge that it is possible unauthorized access may occur, especially given today's environment of rapidly advancing technology. Navy Federal supports assisting members during times of increased likelihood that (1) unauthorized transactions occur on their accounts, and (2) they become victims of identity theft. This proposal would require financial institutions to provide such assistance in certain circumstances, and therefore Navy Federal supports this proposal in concept. However, we would like to offer further comments and suggestions regarding how financial institutions will operationally implement certain aspects of these proposed Guidelines.

Definition of "Sensitive Customer Information"

The proposal defines "sensitive customer information" as a customer's social security number, personal identification number, password, or account number, in conjunction with a personal identifier such as a customer's name, address or telephone number. The proposed definition of "sensitive customer information" also includes any combination of components of customer information that would allow someone to access another person's account, such as a username and password.

Ms. Jennifer J. Johnson

Page 2

October 14, 2003

Navy Federal supports defining the term "sensitive customer information," but also encourages the federal regulatory agencies to include a customer's date of birth and driver's license number, in conjunction with a personal identifier, in the definition. Navy Federal believes many financial institutions commonly use a combination of these items to verify customers' identities, and that a security breach involving customers' dates of birth and addresses, for example, could be just as serious as a security breach involving social security numbers.

Investigation of Unauthorized Access

The proposed Guidance would require a financial institution to notify affected customers of unauthorized access to sensitive customer information if it concludes, after an appropriate investigation, that misuse of the information is likely to occur and takes steps to safeguard the interests of affected customers. Navy Federal appreciates the federal regulatory agencies' flexibility in allowing financial institutions to determine whether customer notice is necessary, and believes that the inclusion of the specific examples at the end of the proposed Guidance as to when notices would and would not be expected are especially helpful. However, Navy Federal is concerned that the requirements of such an "appropriate investigation" could be interpreted differently by various regulators and financial institutions if a particular incident of unauthorized activity does not fall within one of the listed specific examples in the Guidance. Therefore, we encourage the federal agencies to include an even more descriptive, non-inclusive, list of examples at the end of the Guidance.

Account Monitoring

Even if the investigation reveals misuse of the information is *unlikely* to occur, the proposed Guidance would still require the institution to monitor the accounts for unusual activity. Navy Federal believes the specific requirement to monitor such accounts, whether or not the financial institution determines customer notice is necessary, could be particularly burdensome in some situations. For example, Navy Federal has nearly 2.5 million members, and the majority of those members have more than one account. The requirement to monitor so many accounts, especially if the exact sensitive customer information that was accessed could not be affirmatively identified as belonging to a particular set of members' accounts, would be extremely burdensome, and would potentially require more employee time and effort than would be immediately available. In addition, Navy Federal notices that the proposed Guidance neither provides information about what "monitoring" may entail nor provides guidance on how long an institution must monitor any affected accounts.

Navy Federal encourages the federal regulatory agencies to provide financial institutions with the flexibility to determine whether monitoring of specific accounts is necessary or practical. In situations in which a small number of accounts are involved in the security breach, monitoring may be feasible. However, if a large number of accounts are involved, close monitoring of each account for unusual or suspicious activity may simply not be possible. In addition, if the

Ms. Jennifer J. Johnson

Page 3

October 14, 2003

investigation into the security breach reveals that notice to customers is unnecessary, monitoring of accounts may also be unnecessary.

If a financial institution determines that account monitoring is not feasible or unnecessary, Navy Federal would support modifying the Guidance to simply require a financial institution to (1) notify affected customers of the security breach, and (2) provide those customers with options to ensure their accounts are secure. For example, if it is determined that monitoring is unnecessary, Navy Federal would be willing to notify affected consumers of any such security breach and offer to place special passwords on their accounts and/or change their account numbers. In addition, Navy Federal believes consumers have a shared responsibility with financial institutions to monitor the activity on their accounts. Consumers are responsible for reviewing their periodic account statements for unauthorized transactions, and have the option to verify activity on their accounts over the phone with a financial institution representative, online (if the institution offers a "home banking" type product), or in person at a branch location.

Given the unique resources available to each financial institution, Navy Federal urges the federal regulatory agencies to allow institutions to develop their own internal procedures detailing what options (e.g., adding a password, changing account numbers, etc.) they will provide affected customers in their notices, in lieu of or in addition to monitoring those accounts that may be affected. Navy Federal also believes that it is important to remind affected customers of the many ways they can currently verify their account activity in any such notices as well.

Timing of Notice

The proposed Guidance allows financial institutions to investigate any security breach to determine whether customer notice is required. Navy Federal encourages the federal regulatory agencies to clarify that notice would be required within a reasonable time after a financial institution determines whether customer notice would be appropriate.

Implementation Period

Navy Federal strongly encourages the regulatory agencies to consider allowing a lengthy time period for financial institutions to implement this Guidance once it is finalized. Even if account monitoring is not required, contracts with third party service providers would have to be modified to include specific procedures for unauthorized systems access involving "sensitive customer information." In addition, if account monitoring is required, institutions would also have to engage in extensive employee training and possibly data processing modifications. Navy Federal would support a time period of one year or longer after any final Guidance is issued for financial institutions to fully implement these response elements into their information security programs.

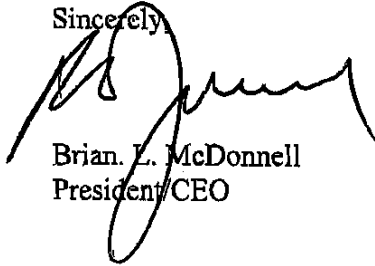
Ms. Jennifer J. Johnson
Page 4
October 14, 2003

Other Comments

Currently, the proposed Guidance would not require financial institutions to notify customers of a breach of information not falling within the definition of "sensitive customer information." Navy Federal supports this flexibility, and encourages the federal regulatory agencies to continue allowing a financial institution the option of notifying affected customers in any other extraordinary circumstances that compel it to conclude that unauthorized access to information, other than sensitive customer information, likely will result in substantial harm or inconvenience to those affected.

Navy Federal appreciates the opportunity to respond to the federal regulatory agencies' request for comments regarding the proposed Guidance on response programs for unauthorized access to customer information.

Sincerely,



Brian L. McDonnell
President/CEO

BLM/slb

cc: Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency
Office of Thrift Supervision